Risk Assessment and Its Impact on VV&A

RPG Special Topic

11/30/00

Table of Contents

What is Risk?

The McGraw-Hill Dictionary of Engineering defines risk as "the potential realization of undesirable consequences from hazards arising for a possible event." There is risk associated with any endeavor in which complete knowledge and control of an outcome is either impossible or impractical, or in which uncertainty is an inherent part of the endeavor. Risk is a factor in any kind of decision-making in which imperfect evidence is used to help make the decision. Two types of risk can be associated with making a decision:

- **Type I** – rejecting correct evidence
- **Type II** – accepting incorrect evidence

In modeling and simulation, the second type of risk, accepting results as correct when they are incorrect, is usually considered more important and is the focus of this discussion.

Risks associated with simulation development and use can be categorized as either **development risk** or **operational risk**.

- **Development risks** are related to the simulation development itself and typically relate to potential problems in meeting technical, schedule, or cost aspects of the simulation development or modification program.
- **Operational risks** are those arising from using the incorrect outputs of a simulation that are believed to be correct.

This document discusses both development and operational risk assessment as a basis for designing VV&A efforts to support simulation development and use. The risks discussed here apply equally to models, simulations, and federations of simulations; however, for simplicity, the term simulation will be used and will apply in all cases.

How Does Risk Impact Simulation?

The primary risk in modeling and simulation is that the simulation will produce an incorrect result or will "fail." By definition, a **failure** can occur only when the simulation is being used for its intended purpose. An incorrect result occurring at any other time (such as during testing of the simulation) would not be a failure[1].

[1] An incorrect result of a model or simulation that occurs during testing or any time other than when the simulation is being used for its intended purpose is deemed an "error."

A failure generally results from some **defect** in the simulation or its operating environment. Although many simulation defects are manifested in either code or data, the source of a defect may well be based on undetected problems that occur at a much earlier stage of the development (e.g., incomplete initial statement or interpretation of a requirement; improper underlying algorithms; inappropriate design) or in a separate component of the simulation (e.g., integration of human-in-the-loop (HITL)). Some defects result from hardware, such as the infamous Pentium floating-point errors ["Pentium II Math Bug," Dr. Dobb's website] or from Developer misunderstandings of such operating conditions as the effects of latency.

Relationship Between Risk and VV&A

Verification and validation activities are designed to discover defects and thus reduce development risk. A V&V effort is also used to accumulate the information needed to support an assessment of operational risk. Accreditation assessment activities are designed to mitigate operational risk.

Simulations inevitably contain defects in their implementation, e.g., in the algorithms and equations, data, or procedures. Many of these defects may go undetected, particularly those that have an insignificant effect on the output of the simulation. It is rarely economical or even possible to uncover and correct all potential defects. Although undiscovered defects reside in any simulation, the seriousness of a potential failure depends both on the application and on the nature of the defect.

The objective of a V&V effort is to uncover as many defects as possible, and in particular, to find all critical defects in order to minimize the risk that the simulation will produce inaccurate results in the given application.

Verification and validation tasks should be carefully selected to focus on the needs of the application, not just on the strengths and weaknesses of the simulation being evaluated. A focused V&V effort can generate evidence to help ensure that critical defects are found and corrected. Furthermore, it can characterize any uncorrected defects so that the operational risk associated with each defect can be assessed during the accreditation assessment. Results of the operational risk assessment should be included in the Accreditation Assessment report.

Example 1:

Consider the case of two potential applications of an air combat training simulation: training pilots to fly low (i.e., as a standard flight training tool) and training pilots to execute a critical mission to bomb a specific target (i.e., as a mission rehearsal tool). Assume that validation results demonstrate that the simulated radar depiction of a power plant is visually acceptable, but that the geographic location of the power plant is off by 1000 meters.

In considering the simulation for the flight training application, the physical location of the power plant is immaterial, and the risk of "negative training" is low. The goal, after all, is to learn to fly low and not hit things, wherever they are. In considering the simulation as a mission rehearsal tool, however, the physical location of the power plant relative to surrounding features is critical. In the actual mission, the pilot would be expecting the target to be in one location but it would actually be somewhere else, with potentially disastrous consequences for pilot safety and mission success.

Risk Management

The various players involved in the VV&A of a simulation have different views of risk management.

- For the User, the ultimate objective is to reduce operational risk to an acceptable level.
- For the M&S program manager (PM) and developer, the objective is to reduce development risk. They seek to ensure delivery of a simulation on time and on or under budget that satisfies the specified requirements.
- For the V&V Agent, the objective is to mitigate development risk by characterizing and classifying potential simulation failures and collecting the evidence needed to demonstrate the capability and fidelity of the simulation.
- For the Accreditation Agent, the objective is to identify, characterize, and manage operational risks by assessing the potential impact of simulation failures upon the specified application and by evaluating evidence that demonstrates the capability and accuracy of the simulation.

The importance of the consequence of a defect is relative. It is based on the defect's impact on the simulation results. Risk management should be guided by two fundamental principles:

- A defect is of consequence if it can lead to a failure
- The value of the defect is directly related to the potential cost of the failure

Development Risk Assessment

Simulations are built or modified to satisfy a set of M&S requirements: a collection of conditions, standards, and values that define the needs of an application. One of the primary development risks is that the simulation will not meet these requirements. To assess development risk, the requirements should be traced to the components of the simulation or federation (e.g., data, humans-in-the-loop, hardware-in-the-loop, software federates) that contribute to, or influence, the fulfillment of those requirements. The goal is to determine which components contribute to the satisfaction of a specific requirement. This does not require a detailed analysis of the significance of the component's contribution; it should be sufficient to simply determine if the component is related to a requirement or not.

Important considerations for assessing development risk include:

Development Risk Questions
• What is the impact if a defect results in a failure to satisfy a requirement?
• What is the probability that a defect will cause such a failure?
• What is the likelihood that a defect will occur?
• Does the simulation operate as required under all conditions matching the intended use?

There are many risk assessment techniques. Two such techniques are discussed in MIL-STD-882C [1993]. Although this standard has been updated and no longer describes the techniques below, these techniques are still applicable to VV&A.

- **Failure Modes and Effects Criticality Analysis** (FMECA) -- an analysis tool from the aerospace industry. This technique examines the dimensions of failures and the effect of those failures on the system and then combines the two components into a criticality value that is literally a measure of how important a failure is. Although this measure is inexact, it is useful.
- **Failure Modes and Impacts Criticality Analysis** (FMICA) – a variant of FMECA that distinguishes between the **effect** of a failure (e.g., dramatic but inconsequential; subtle but disastrous) and the **impact** of a failure (a measure of its undesirability to the problem at hand).

In assessing simulation risk, FMICA is more applicable than FMECA. The following paragraphs present the process for conducting a FMICA for a simulation.

FMICA Simulation Assessment Process

The FMICA process is based on the premise that an impact is associated with the failure of the simulation to meet any requirement. For some requirements (e.g.,

requirements defining fidelity or data quality), the severity of the impact may be a function of the quality or degree of the failure. The FMICA process involves two main sub-processes: impact assessment (**IA**) and failure mode identification (**FMI**).

Impact Assessment Process

The FMICA process begins with a four-step impact assessment. Note that results of the impact assessment can be used to support phasing decisions of a large project without completing the failure mode or criticality assessment parts of the FMICA.

The User is normally in the best position to assess the severity of the impact of a failure. Impact assessments involving hundreds of requirements can be performed (and performed well) in just a day or two by one knowledgeable user. Even if the user does not perform the assessment, a complete initial impact assessment should not involve more than a few people or take more than a workweek to complete.

IA Step 1. Determine a set of categories that define specific failure impacts

The impacts of each category should be defined in problem-specific terms, not as high, medium, or low. Generally from three and seven different categories are used. Many category failure impact descriptions can be of equivalent impact. The set should not be rank-ordered.

Example 2: A preflight planning simulation might use a set of failure impact categories such as these.

Failure Impact Categories

Category	Impact
A	• Results in flight plans that cannot be followed and that are unlikely to be corrected in flight
B	• Results in flight plans that require significant experience to correct in flight
C	• Results in flight plans that probably can be corrected in flight by an average pilot.
D	• Results in flight plans that are easily corrected by any pilot
E	• Results in flight plans in which the errors have no impact on the conduct of the flight

These categories identify adverse impacts, not positive impacts. If a failure causes a positive impact, the validity of the requirement or the correctness of the simulation implementation should be examined.

IA Step 2. Associate a category with each M&S requirement

By definition, failure of the simulation to meet a requirement typically has an impact on the output of the simulation. The level of impact of this failure may depend on how well or poorly the requirement is met as shown in example 3. Requirements for fidelity of

certain representations may need to be decomposed because individual elements of the representation may result in different failures and consequently different impacts on simulation outputs. In addition, the effects of failure may differ depending on the degree of failure involved.

> Example 3:
>
> In the power plant example (example 1), failure to meet a requirement that "power plant location must be accurate to within 100 meters" may be categorized as a **D** if the location is only 30 meters off and the plant is located in an undeveloped area. However, it might be a **B** or even an **A** if the location is 300 meters off and the plant is in an area with several nearby radar-significant targets.

If the vast majority of impacts fall into a single category, then the category definitions should be reconsidered.

IA Step 3. Obtain User approval of the impact category assignments

The user is uniquely qualified to assess the severity of the impact of a failure. Normally, the user conducts the entire IA process and this step is axiomatic. However, if an outside agent, e.g., the V&V or accreditation agent, is designated to perform the impact assessment, it is important that the User review and approve all impact category assignments to ensure they accurately reflect the user perspective. Additionally, the user can seek out subject matter experts (SMEs), the developer, and other agents if additional expertise is needed.

IA Step 4. Reevaluate the impacts of modified and new requirements

The impact assessment should be accomplished for the complete set of M&S requirements. For a new development, the impact assessment should be completed before the design phase is complete. When requirements are modified or when new requirements are added, their impact should be assessed. This assessment should include possible ripple across other requirements even though each requirement is considered independently and there is no rank ordering.

The IA process results in a categorized list of requirements with the most likelihood of having failures associated with them. This list can help the M&S PM, developer, and V&V and accreditation agents better understand simulation requirements. The M&S PM and developer can use this information to design the development effort, and the V&V and accreditation agents can use it to scope the V&V and accreditation efforts.

Failure Mode Identification Process

The failure mode identification (FMI) process is the second half of FMICA. In this process, simulation defects are separated into four failure mode classes based on the source of the defect involved:

- requirement failures
- algorithm and data failures
- software implementation failures
- support component failures

Additional information about failure mode categories is available in Appendix A

FMI should be performed by a team with expertise in the details of the simulation implementation. This team should include the developer, user, SMEs, V&V agent and accreditation agent.

The FMI process involves five basic steps.

FMI Step 1. For each requirement, identify those simulation system components with a role in implementing the requirement

The level of decomposition detail depends on factors such as whether the software is newly developed or legacy software, whether it includes support components (e.g., human-in-the-loop), etc.

- For newly developed software, the software component or object package level is an appropriate decomposition level.
- For legacy software[2], the decomposition detail depends on the documentation available and the similarity between the current and previous applications. At one extreme, the decomposition may be similar to the development case where no documentation exists or where existing software will be extensively modified. At the other extreme, if previous users completed this decomposition, a simple review of that documentation is all that is needed.

FMI Step 2. Establish a set of categories that encompass the likelihood of failure

Three to seven categories are generally sufficient. The categories should be defined according to a set of criteria into which it is relatively easy to place the specific simulation.

[2] This includes commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) software.

Example 4:

A set of categories for a stand-alone simulation (no additional components) might include these categories.

Sample Failure Mode Categories	
Category	**Definition**
A	Developmental software with algorithm complexity pushing the state of the art
B	Developmental software of a routine character
C	Developmental software with complex data structures requiring data difficult to assess for quality
D	COTS package widely distributed and used within intended purposes
E	Vertical market COTS/GOTS with limited user base.
F	Hardware-in-the-loop from a developmental system
G	Hardware in the loop from an operational system

FMI Step 3. Rank-order the categories

Unlike the categories defined for impacts (shown in example 2), failure mode categories should be rank-ordered, but only after they have been completely defined. The defect likelihood ranking for the set of categories shown in example 4 might be:

A > C > E > F > B > G > D

FMI Step 4. Assign each component appearing in the requirements decomposition (FMI Step 1) to a failure category (FMI Step 2)

This step results in a listing of all the components or object packages that are Category A failure candidates, then those that are Category B failure candidates, and so forth. Although this does not specify the exact failure mode to be expected, it does indicate a general area to be observed; e.g., if a particular component is identified as a possible candidate for failure Category C, the analyst would concentrate on observing the behavior of the complex data relationships within that component or object package. Note that Category C was the second most likely failure mode to occur according to the rank ordering in the example, which indicates a fairly high likelihood of failure.

FMI Step 5. Obtain consensus from all participants (e.g., SMEs, Developer, User, V&V Agent) as appropriate

This step provides a categorized list of those system components that support a critical requirement and that have the most likelihood of having failures associated with them. This list can help the M&S PM and developer better understand which components to spend the most effort on quality assurance. The V&V and accreditation agents can also use this information to focus the VV&A effort on the most critical components.

Development Risk Mitigation

The criticality of a failure to satisfy a specific requirement is some combination of the impact of the failure and the likelihood that the failure will occur. The specific combination of impact and occurrence depends on the application. An approximate level of criticality can usually be assigned to each requirement for a specified application. A rank-ordering of the requirements by level of criticality is generally unnecessary; grouping them into categories, which are in turn rank-ordered, should be sufficient.

In many cases, this categorization will be obvious. Requirements that result in a severe impact on the results if they fail or that have a high likelihood of containing a defect in their implementation can be identified as being highly critical. Conversely, a requirement whose failure has minimal impact and that is implemented in components with little likelihood of containing a defect is considered not very critical.

Various methods can be used to assign numerical values to the importance or criticality of a requirement by combining the severity of the impact with the likelihood of a defect. Example 5 is a sample of the criticality scoring process based on the FMICA technique.

Example 5:

1. **Assign an impact score to each Failure Impact Category** (see example 2).

   Duplicate values are allowed.

   Different methods can be used, such as rank of the category or square of the rank of the category.

   Each member of the category is assigned the impact score of the category.

2. **Within each Failure Impact Category, assign a score to each requirement based on its individual Failure Mode Category** (example 4**) and rank-order the categories.**

   The rank can be used as the score.

3. **Assign criticality scores to each requirement.**

   For each requirement, inspect the list of components involved and select the component with the most severe failure mode score for that requirement.

   Calculate the product of the impact and the failure mode scores of that component and assign it as the criticality score for the requirement.

4. **Order the requirements by their criticality scores**

   Examine the ordering and the scores for gaps. Where score gaps exist, make them the boundaries between criticality categories. Otherwise assign boundaries arbitrarily. Give due consideration to criticality scores whose value has a disparity between the failure mode and the impact score

The process in example 5 shows how to develop a rank-ordered list of the requirements that are critical if they fail and how to determine the likelihood that the component or components that support a given requirement may fail. This allows the V&V Agent to concentrate the V&V activities on observing those components as they are developed

or modified and tested. In cases where V&V resources are constrained, this technique enables the V&V Agent to focus on the most critical simulation components.

Operational Risk Assessment

Operational risk has to do with credibility. Whereas M&S requirements establish what the simulation must do and how well it must be done, credibility drives how much information is needed about the simulation to make a reasonable and acceptable accreditation decision. The User needs to believe that the simulation results are "good enough" to use.

The amount of confidence that the User needs in the results of the simulation depends on how much risk the User is willing to tolerate. Such a question is often difficult to answer because Users seldom overtly specify risks, particularly in concrete, quantifiable terms. Therefore, to define necessary confidence levels, a means of identifying and quantifying risks is needed. The first step is to answer some detailed questions, including:

Operational Risk Questions
• What risks would result from an incorrect decision that is based on simulation outputs?
• What is the nature of those risks (safety, financial, unit effectiveness, program jeopardy, etc.)?
• What organizations or groups might be affected by these risks?
• What is the likelihood that an incorrect decision or outcome will result if the model produces erroneous outputs or predictions?
• What visibility will an incorrect decision have?
• Does the User have any specific issues or concerns that should be considered as risks?

Answers to these questions provide the essential ingredients for the operational risk analysis (ORA) process described below. This risk analysis process follows the methodology outlined in MIL-STD-882D [2000], the standard for system safety.

Operational Risk Analysis

Assessment Considerations

Risk is made up of two components: the impact (or consequences) of an event and the probability of the event's occurrence.

If each of these components could be quantified, the level of risk could be expressed using the formula:

Risk = (Impact Level) x (Probability of Occurrence)

In many cases, the factors in this equation cannot be quantified absolutely but can be subjectively estimated using the principles in the referenced standard [MIL-STD-882D, 2000].

ORA 1: Quantify Impact Level

The first step in the operational risk analysis is to quantify the impact level. MIL-STD-882D divides the impact into four levels: catastrophic, critical, marginal, and negligible. The criteria for assigning one of these impact levels to a particular risk is subjective, but can be made explicit. MIL-STD-882D also provides criteria for determining impact levels for risks related to personnel and equipment safety, environmental damage, and occupational illness. Criteria for some additional categories (e.g., impact on end-user capability or effectiveness, cost, performance, schedule, and political or public reaction) have been added. A suggested set of criteria for determining impact levels is given in the table below. This table expands the criteria found in MIL-STD-882D for the safety categories by adding parallel criteria for additional categories.

Criteria for Determining Impact Severity				
Impact Categories	**Impact Levels**			
	CATASTROPHIC	**CRITICAL**	**MARGINAL**	**NEGLIGIBLE**
Personnel Safety	Death	Permanent Partial Disability	Injury resulting in 1 or more lost work days	Minor injury with no lost work days
Equipment Safety	Major equipment loss; broad-scale major damage	Small-scale major damage	Broad-scale minor damage	Small-scale minor damage
Environmental Damage	Irreversible & severe damage	Reversible damage $200K< loss < $1M	Damage $10K< loss < $200K	Damage <$10K not violating laws or regulations
Occupational Illness	Severe & broad scale	Severe or broad scale	Minor & small scale	Minor or small scale
Cost	Loss of program funds; 100% cost growth	Funds reductions; 50-100% cost growth	20-50% cost growth	< 20% cost growth
Performance	Design does not meet critical thresholds	Severe design deficiencies but thresholds met	Minor design flaws, but fixable	Some trivial “out of spec” design elements
Schedule	Slip reduces overall DoD capabilities	Slip has major cost impacts	Slip causes internal turmoil	Slip causes schedules to be republished

Criteria for Determining Impact Severity				
Impact Categories	**Impact Levels**			
	CATASTROPHIC	**CRITICAL**	**MARGINAL**	**NEGLIGIBLE**
Political Or Public Impact	Widespread (Watergate)	Significant (Tailhook '91)	Embarrassing ($200 hammer)	Local

ORA 2: Quantify probability of occurrence

The other factor in the risk equation is the probability that the event causing an impact will occur. The expected number of occurrences of a given event contributing to risk can be described in one of four ways, depending on the type of risk factor being considered:

- over the life of a system
- per number of items in a population
- per unit of time
- per number of events

MIL-STD-882D [2000] divides the probability continuum into five bands and gives guidelines for selecting the appropriate band. The probability level table below provides these guidelines in terms of the number of occurrences during the lifetime of an item and the number of items in a population. However, these guidelines can be extrapolated to address other types of impacts that can be experienced over time or over a number of events.

Probability Levels*		
Probability Continuum	**Likelihood of Occurrence over Lifetime of an Item**	**Likelihood of Occurrence Per Number of Items****
Frequent	Likely to occur frequently	Continuously experienced
Probable	Will occur several times in life of item	Will occur frequently
Occasional	Likely to occur some time in life of item	Will occur several items
Remote	Unlikely but possible to occur in life of item	Unlikely but can reasonably be expected to occur
Improbable	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur but possible
* Extracted from MIL-STD-882D [2000]. ** Number of items should be specified.		

Once the severity of the impact and its probability of occurrence have been quantified, the level of risk (which is directly related to the required level of credibility) can be determined. The sample risk assessment matrix below, based on MIL-STD-882D

[2000], relates the level of risk to different levels of impact and probabilities. Because the risks associated with using a specific simulation in a given application will be unique, the risk assessment matrix should be developed based on the User's perception of risk.

Sample Risk Assessment Matrix*				
Frequency	**Level of Impact**			
	CATASTROPHIC	**CRITICAL**	**MARGINAL**	**NEGLIGIBLE**
Frequent	High	High	Medium	Low
Probable	High	High	Medium	Low
Occasional	High	Medium	Low	Low
Remote	Medium	Medium	Low	Low
Improbable	Medium	Low	Low	Low
* Based on sample in MIL-STD-882D [2000].				

This process should be repeated for every particular risk factor. The highest risk level among all the factors determines the degree of confidence needed. The subjective criteria used in each step of this process are all explicitly stated and should be tailored to the specifics of individual problems. The explicit statement of subjective criteria is advantageous because it allows the criteria to be easily discussed and agreed upon by consensus of the group.

Operational Risk Mitigation

The level of operational risk determined through the assessment techniques just described is the basis for determining the type, quality, and depth of information that is needed to support the accreditation decision. The higher the level of operational risk, the greater the User's need for specific, detailed information that describes the simulation's ability to produce acceptable results in the specified application. By satisfying this need for information, the V&V and Accreditation Agents can help the User build confidence that the simulation outputs are credible for the intended application and thus mitigate the operational risks associated with the intended use.

Conclusion

Risk analysis provides a specific, objective, and frequently quantitative method for identifying potential problems associated with the development and application of a simulation for a particular purpose. It helps the M&S PM and the V&V and Accreditation Agents focus V&V activities on the critical parts of the simulation.

Using risk assessment techniques, the scope of the V&V and accreditation efforts necessary to achieve an appropriate (acceptable) risk can be estimated and appropriate

trade-offs made. In addition, the V&V and accreditation efforts can be directed toward the most effective risk mitigation program possible with the available resources.

References

Grey, Stephen, *Practical Risk Assessment for Project Management*, June 1995.

Jones, T. Capers, *Assessment and Control of Software Risks*, Yourdon Press Computing, February 1994.

Molak, Vlasta (Ed.), *Fundamentals of Risk Analysis and Risk Management*, November 1996.

Muessig, P.R., Laack, D.R., and Wrobleski, J.J., "Optimizing the Selection of VV&A Activities, A Risk/Benefit Approach," *Proc. 1997, Summer Simulation Conference*, Arlington, VA, pp. 855-860.

Parker, S. P. (Ed.), *McGraw-Hill Dictionary of Engineering*, 5th edition, McGraw-Hill, New York, NY, 1997.

External Links in this Document

MIL-STD-882C: *System Safety Program Requirements, Appendix A: Guidance for Implementation of System Safety Program Requirements*, Jan 1993. Standards website for Florida Chapter System Safety Society: http://www.afmc.wpafb.af.mil/organizations/HQ-AFMC/SE/ssd.htm

MIL-STD-882D: *System Safety Program Requirements, Appendix A: Guidance for Implementation of System Safety Program Requirements*, Feb 2000. Defense Automation and Production Service website: http://astimage.daps.dla.mil/quicksearch/

"Pentium II Math Bug?" Dr. Dobb's Microprocessor Resources website: http://x86.ddj.com/secrets/dan0411.htm.

RPG Links in this Document

RPG Reference Document: "Credibility"

RPG Special Topic: "Fidelity"

RPG Special Topic: "Requirements"

RPG Special Topic: "Subject Matter Experts and VV&A"

Appendix A: Failure Modes

Failure Mode Identification is the second subprocess within the **Failure Modes and Impacts Criticality Analysis** (FMICA) process described in MIL-STD-882C [1993]. In order to identify potential failure modes, it is first necessary to understand the various types of failures that can occur during development and use of a simulation.

Simulation defects fall into four failure mode classes based on the source of the defect involved (i.e., misstatement, misinterpretation, or omission of a requirement; definition of the underlying algorithms and data; software implementation; support components of the simulation system):

- **requirement failures --** Misunderstandings regarding requirements are most likely to be identified during requirements verification or conceptual model validation. During new simulation development, requirements tracing throughout the development process can help identify related problems before they become failures. When a legacy simulation is involved, the User compares the requirements of the current application with the capabilities of the selected legacy simulation to determine if there are any inconsistencies or inadequacies. Tools that can perform comprehensive requirements tracing can facilitate this task.
- **algorithm and data failures --** The algorithms used to generate specific results, such as attrition algorithms, path generators, etc., and their associated data (both hard-wired data and input instance data) need to be accurate and of an appropriate level of fidelity.

  Example: An algorithm that calculates attrition based on single shot kill probability may be appropriate for determining the results of a platoon-level tank battle but it would be inappropriate for use in a simulation that is assessing the results of a corps-level battle.

  Subject matter experts (SMEs), including data producers, should be involved in assessing the likelihood of failure. Other algorithm failures may involve a mismatch between statistical distributions or sampling in the new simulation.
- **software implementation failures --** The Developer is normally in the best position to identify which system components or algorithms may cause the simulation to fail to meet a requirement during execution. For a legacy simulation, good software documentation is essential for providing this information.

- **support component failures --** When considering support components, (e.g., human-in-the-loop (HITL)[3], hardware-in-the-loop (HWTL) networks, interface devices, post processors, analysts, operators), a variety of factors may contribute either directly or indirectly to the simulation's inability to satisfy a requirement. Simulation domain SMEs may be needed to identify these potential factors and estimate the likelihood of failure.

> Example:
>
> When humans are involved, either as HITL, operators, or analysts, failures may result from such factors as incomplete training, fatigue, team inexperience, stressful physical environment, or lack of rehearsal.

References

External Links in this Appendix

MIL-STD-882C: *System Safety Program Requirements, Appendix A: Guidance for Implementation of System Safety Program Requirements*, Jan 1993. Standards website for Florida Chapter System Safety Society: http://www.afmc.wpafb.af.mil/organizations/HQ-AFMC/SE/ssd.htm

RPG Links in this Appendix

select menu*:* *RPG Reference Documents*, select item: "M&S Data Concepts and Terms"

select menu*:* *RPG Special Topics*, select item: "Subject Matter Experts and VV&A"

The appearance of hyperlinks does not constitute endorsement by the DoD, DMSO, the administrators of this web site, or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the DoD does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DMSO web site.

§ § § § § § §

[3] HITL are frequently relied on to provide decision-making either as they would in the real world or as integrated parts of the simulation (i.e., as operators of semi-automated forces or warfighters interacting with a new weapon system concept). In either situation, HITL performance can result in simulation failure; the participants can either make incorrect decisions or provide responses incorrectly to the simulation.